IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

ERIK LASALLE, *on behalf of himself and all others similarly situated*,	:	
	:	**CIVIL ACTION**
v.	:	**No. 25-974**
	:	
ADOPTIONS FROM THE HEART, INC.	:	

McHUGH, J. **August 1, 2025**

MEMORANDUM

This is a data breach case. In April 2024, an adoption agency inadvertently exposed the sensitive personal data of over 2,000 present and former clients. The data remained publicly accessible on the internet for a nine-day period before it was taken down, and the agency failed to notify any impacted parties for nine months. Soon after his data was exposed, Erik LaSalle, a former client, experienced a spike in spam communications and attempted bank fraud. Mr. LaSalle now brings a putative class action for both monetary and injunctive relief on behalf of himself and the other individuals whose data was compromised. Defendant has moved to dismiss for lack of standing, arguing that Plaintiff has not experienced injuries fairly traceable to the data incident. I disagree. In an era of data mining by sophisticated programs, once information is made public on the internet, even if only for a few days, the vulnerability is real. Here, Plaintiff has sufficiently alleged that he is both at risk of, and has already begun to experience, serious harms that plausibly flow from the data incident. The motion to dismiss will therefore be denied.

I. Facts as Pled

Defendant Adoptions from the Heart, Inc. is a non-profit adoption agency. Compl. ¶¶ 9, 13, ECF 11. In running its business, Defendant receives and maintains adoption files containing personal identifiable information ("PII") and protected health information ("PHI") of thousands of

its current and former clients. *Id.* ¶ 14. Some of this information includes names, dates of birth, social security numbers, medical records, and names of social workers. *Id.* ¶ 3. In agreeing to work with Defendant, clients sign a Privacy Policy, wherein Defendant promises not to share the PHI or PII with anyone outside of the Agency. *Id.* ¶ 17.

Despite this assurance, on April 17, 2024, the data stored in Defendant's internal database was made available and searchable on the internet ("the Incident"). *Id.* ¶ 18. At least 2,502 of Defendant's former patients and clients' data files were exposed, and the data remained public for nine days. *Id.* ¶¶ 4, 22. During this period, the data was susceptible to search engine indexing bots, which are automated data harvesting mechanisms designed to crawl the internet for publicly accessible data. *Id.* ¶ 19. Such bots often facilitate large-scale automated data scraping, a known exploitation method used by cybercriminals and data brokers to capture sensitive personal information at scale. *Id.* ¶ 20. Personal data collected through web scraping is frequently sold or published on the Dark Web.[1] *Id.* ¶ 35. Plaintiff asserts that "on information and belief," the PII/PHI data jeopardized in the Incident has already been made publicly accessible and has been published, or will be published imminently, by cybercriminals on the Dark Web. *Id.* ¶ 36.

Yet, Defendant did not notify affected parties of the Incident until January 24, 2025 – over nine months after the exposure. *Id.* ¶ 23. This dramatic delay limited the ability of affected parties to try to mitigate their injuries in a timely manner.[2] *Id.* ¶ 24.

[1] The Harvard Business Review describes the Dark Web as a "hub of criminal and illicit activity" where cybercriminals "sell data from companies they have gained unauthorized access to through credential stuffing attacks, phishing attacks, [or] hacking." Compl. ¶ 35; Brenda R. Sharton, *Your Company's Data Is for Sale on the Dark Web. Should You Buy It Back?*, HARVARD BUS. REV. (Jan. 4, 2023) https://hbr.org/2023/01/your-companys-data-is-for-sale-on-the-dark-web-should-you-buy-it-back.

[2] In their Notice, Defendant offered to provide some victim credit monitoring and identity related services. *Id.* ¶ 31. But this offer carries little import when it was not made until over nine months had lapsed, for time is of the essence when attempting to mitigate a data breach.

Plaintiff Erik LaSalle is a former client of Defendant, and thus provided the Agency with his PII and PHI, trusting that the Agency would use reasonable measures to keep his information safe. Plaintiff "is very careful about the privacy and security of his PII/PHI," "does not knowingly transmit his PII/PHI over the internet in an unsafe manner," and is careful to store any sensitive documents in a secure location. *Id.* ¶ 40. But in February 2025, LaSalle received notice that his data file was one of those exposed in the Incident. *Id.* ¶ 45.

LaSalle avers that following the Incident, he experienced a spike in spam and scam text messages and phone calls. *Id.* ¶ 47. Within a year of the Incident, LaSalle also asserts that he received a call from Capital One informing him that an unauthorized actor had made several attempts to withdraw money from his account. Capital One consequently froze his account, which he then decided to close. *Id.* ¶ 46. LaSalle believes that these episodes of fraudulent activity are a product of the Incident. To this point, LaSalle does not recall ever learning that his information was compromised in any other data security incident, other than the Incident at issue here, leading him to infer that as a result of the Incident and the widespread prevalence of indexing bots, his information was compromised and accessed by nefarious third parties. *Id.* ¶¶ 44, 49.

In addition to the spam calls and attempted bank fraud, LaSalle states that he has spent, and will continue to spend, significant time, effort, and money monitoring his accounts to protect himself from identity theft. *Id.* ¶¶ 51, 62. He avers that he has suffered from anxiety, sleep disruption, stress, fear, and frustration. *Id.* ¶ 53. He also alleges a loss of opportunity costs and wages from spending time trying to mitigate the fraud, and an ongoing risk of additional data breaches until Defendant takes appropriate protective measures. *Id.* ¶ 62.

Plaintiff purports that Defendant knew or should have known that a failure to safeguard sensitive data presents great risk, but that they nevertheless failed to take adequate precautions,

follow statutory or industry standards, or sufficiently notify affected parties once aware of the Incident. *Id.* ¶¶ 77, 83, 84, 86, 90.

LaSalle brings this suit as a class action on behalf of himself and a similarly situated class consisting of "all individuals residing in the United States whose PII/PHI was compromised and/or made accessible to internet search engines as a result of the indexing error discovered by Adoptions From The Heart in April 2024, including all individuals who received a Notice of Security Incident." *Id.* ¶ 92. Defendant does not dispute that the Incident occurred, nor that they failed to notify putative Plaintiffs for nine months. Defendant argues instead that Plaintiff cannot establish a causal connection between the Incident and Plaintiff's alleged fraud, warranting dismissal for lack of standing.

II. Standard of Review

Defendant argues that the action should be dismissed for lack of subject matter jurisdiction pursuant to Rule 12(b)(1). A challenge to subject matter jurisdiction under Rule 12(b)(1) may be either a facial or factual attack. "A facial attack, as the adjective indicates, is an argument that considers a claim on its face and asserts that it is insufficient to invoke the subject matter of the court[.]" *Const. Party of Pa. v. Aichele*, 757 F.3d 347, 358 (3d Cir. 2014). In contrast, a factual attack is "an argument that there is no subject matter jurisdiction because the facts of the case . . . do not support the asserted jurisdiction." *Id.* In both instances, the plaintiff bears the burden of establishing subject matter jurisdiction. *Kehr Packages, Inc. v. Fidelcor, Inc.*, 926 F.2d 1406, 1409 (3d Cir. 1991).

The jurisdictional challenge here is a facial challenge to standing. As such, I must "accept the Plaintiff's well-pleaded factual allegations as true and draw all reasonable inferences from those allegations in the Plaintiff's favor." *In re Horizon Healthcare Servs. Inc. Data Breach Litig.*,

846 F.3d 625, 633 (3d Cir. 2017) (cleaned up). Where, as here, Plaintiff brings a class action, only one Named Plaintiff must have standing for the matter to proceed. *Id.* at 634.

III. Discussion

A federal court may only exercise jurisdiction where there is a live "case" or "controversy." U.S. Const. art. III, § 2. For a lawsuit to satisfy that requirement, plaintiffs must have standing to sue. *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992). To establish Article III standing, a plaintiff must show (1) that he suffered an "injury in fact"; (2) that the injury is "fairly traceable to the challenged conduct of the defendant"; and (3) that the injury would likely be redressed by a favorable judicial decision. *Spokeo, Inc. v. Robbins*, 578 U.S. 330, 338 (2016). Defendant only contests the first two elements.

A. Plaintiff demonstrates injury-in-fact.

To qualify as an injury in fact, the injury must be (a) actual or imminent, not conjectural or hypothetical, and (b) concrete and particularized. *Spokeo*, 578 U.S. at 339 (quoting *Lujan*, 504 U.S. at 560); *Adam v. Barone*, 41 F.4th 230, 234 (3d Cir. 2022). Both the actual injuries that Plaintiff has already incurred and Plaintiff's concerns about the ongoing threat of identity theft satisfy these requirements.

1. Actual or Imminent

To have standing, a plaintiff must allege an actual or imminent injury. An actual injury is "a concrete loss as the result of [the defendant's] actions." *Taliaferro v. Darby Twp. Zoning Bd.*, 458 F.3d 181, 190 (3d Cir. 2006). By contrast, a claim of future injury can be "imminent" if there is a "substantial risk" that the threatened harm will occur. *Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 158 (2014) (quoting *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 414 n.5 (2013)). While

a risk of future injury might suffice to establish injury-in-fact, that risk of injury cannot be hypothetical or speculative. *Clemens v. ExecuPharm Inc.*, 48 F.4th 146, 153 (3d Cir. 2022).

Once private data is released to the public on the internet, even if only for a brief spell, it is exceedingly difficult, if not impossible, to control what happens to that data downstream. The Third Circuit has recognized that the unique character of data breach claims makes them likely to present a serious risk of imminent harm, explaining that it is "critical" that "actual or imminent" is disjunctive: "it indicates that a plaintiff need not wait until he or she has *actually* sustained the feared harm in order to seek judicial redress, but can file suit when the risk of harm becomes imminent. This is especially important in the data breach context, where the disclosure of the data may cause future harm as opposed to currently felt harm." *Id.* at 152 (emphasis in original).

Two cases bookend the landscape of the injury-in-fact inquiry in the Third Circuit as it relates to data breaches. In *Reilly v. Ceridian Corp.*, where plaintiffs alleged that hackers *may have* accessed their law firm's payroll system and the sensitive data contained therein, the Court held that the plaintiffs failed to establish injury in fact. 664 F.3d 38 (3d Cir. 2011). Critically, the *Reilly* plaintiffs did not allege any misuse of their data, and based their claim entirely on the possibility that *if* a hacker came across the leaked data, they *could* use it to engage in identity theft. The Court concluded that the future injuries alleged were entirely speculative and declined to find standing. *Id.* at 42.

Over a decade later, and amidst the ever-growing ubiquity of our digital footprints and our greater understanding of its pitfalls, the Third Circuit decided *Clemens*. There, the Court held that a plaintiff sufficiently established injury-in-fact where employee addresses, social security numbers, banking and financial account numbers, insurance and tax information, and more, were stolen during a ransomware attack on the defendant-company's system. *Clemens*, 48 F.4th at 156.

In its analysis, the Third Circuit presented three non-dispositive factors to consider when evaluating whether an alleged injury in the data breach context is sufficiently imminent to satisfy Article III. First, standing is supported where the data breach was intentional and where known hackers or ransomware can be identified. Second, allegations of misuse weigh in favor of standing.[3] And third, courts should consider the sensitivity of the information accessed. "[D]isclosure of social security numbers, birth dates, and names is more likely to create a risk of identity theft or fraud," than instances where financial information without corresponding PII is disclosed, as financial information alone "generally cannot be used to commit identity theft or fraud." *Id.* at 154 (citing *McMorris v. Carlos Lopez & Assoc., LLC*, 995 F.3d 295, 302 (2d Cir. 2021) and *In re SuperValu, Inc.*, 870 F.3d 763, 770-71 (8th Cir. 2017)).

Based on the three factors, the Court determined that the claims in *Clemens* were distinguishable from those in *Reilly* and allowed the case to proceed. First, while it was unclear in *Reilly* whether anyone had accessed the exposed data, the *Clemens* plaintiff identified a known ransomware attacker. Second, unlike in *Reilly*, where the Court could not discern any harm that flowed from the data breach at issue, the plaintiff in *Clemens* asserted that her information had already been distributed on the Dark Web. And while she did not point to any uptick in fraudulent activity, the *Clemens* plaintiff alleged that misuse of her data was either already afoot or would soon manifest. Third, the *Clemens* Court determined that the information at issue was precisely the sort of sensitive information that would lend itself to identity theft – birth dates, social security numbers, and names – weighing in favor of standing as well. *See id.* at 156 (while potential identity

[3] The Third Circuit was careful to qualify that standing might also exist without alleged misuse where there is a clear increased risk of future harm that a plaintiff would not have otherwise faced. *See Clemens*, 48 F.4th at 154 (discussing *Pisciotta v. Old Nat'l Bancorp*, 449 F.3d 629, 634 (7th Cir. 2007)).

theft mitigation could involve "changing one's banking information," "there is no guarantee that mitigative measures will be effective – especially given that some information, such as our names and social security numbers, generally stay with us for life."). Moreover, the Third Circuit held that a meaningful threat of identity theft was sufficiently imminent, supporting a finding of injury-in-fact.

While the facts alleged here differ from *Clemens* on the first factor, this case is still closer to *Clemens* than *Reilly*. Admittedly, Plaintiff does not assert that the data breach was "intentional" and cannot identify a specific hacker or ransomware, beyond articulating the high likelihood that web scraping bots indexed the data while it was publicly accessible. But this factor is not dispositive.

Plaintiff clearly alleges misuse that precipitated from the breach – namely, the noteworthy surge in spam communications and the attempted bank fraud.[4] Plaintiff's allegations of misuse are actual injuries that support standing. *See Roma v. Prospect Med. Holdings, Inc*., No. 23-3216, 2024 WL 3678984, at *6 (E.D. Pa. Aug. 6, 2024) (holding that allegations of ongoing identity theft are actual injuries that support standing without needing to also find imminence); *see also In re Am. Med. Collection Agency, Inc. Customer Data Sec. Breach Litig*., No. 19-2904, 2021 WL 5937742, at *8 (D.N.J. Dec. 16, 2021) (same); *cf. In Re. Retreat Behav. Health, LLC*, No. 23-26, 2024 WL 1016368, at *3 (E.D. Pa. Mar. 7, 2024) (granting motion to dismiss where plaintiff did not allege that their data was misused or published, and thus failed to show imminence).

[4] The alleged misuse also supports an inference that Plaintiff's data was in fact scraped while it was public, making the risk of additional future harm more likely and supporting a finding of imminence on Plaintiff's future harm claims.

Finally, the information at issue is precisely the sort of sensitive information contemplated in *Clemens* that creates a substantial risk of identity theft if publicized. Plaintiff alleges that names, birthdays, and social security numbers, as well as other PHI and PII, were compromised in the Incident. It is difficult to conceive of data more sensitive, as this personal information seldom changes, and can be used to unlock troves of additional sensitive data and accounts. Plaintiffs' injuries are thus "actual" or "imminent."

2. Concrete

A concrete injury is real, not abstract. *TransUnion LLC v. Ramirez*, 594 U.S. 413, 424 (2021). Intangible injuries and harms that are difficult to prove or measure can also be concrete. *Spokeo*, 578 U.S. at 340-41. Certain intangible harms lend themselves to a finding of concreteness. In *TransUnion v. Ramirez*, the Supreme Court explained that "central to assessing concreteness is whether the asserted harm has a 'close relationship' to a harm 'traditionally' recognized as providing a basis for a lawsuit in American courts." *Ramirez*, 594 U.S. at 417. These harms "include, for example, reputational harms, *disclosure of private information*, and intrusion upon seclusion." *Id.* at 425 (emphasis added).

Where a Plaintiff seeks both injunctive and monetary relief, the risk of future harm alone can be concrete, if the risk is sufficiently imminent and substantial. *Clemens*, 48 F.4th at 155 (citing *Ramirez*, 594 U.S. at 435). And where the claimed injury is exposure to a substantial risk of future harm, a plaintiff can show concreteness by alleging the future harm caused "currently felt concrete harms."[5] *Id.* at 155-56.

[5] A claim for damages alone requires a more significant showing that includes extant harms, such as costs spent on mitigation measures or emotional distress requiring medical care. *Clemens*, 48 F.4th at 155.

Here, Plaintiff pleads the *Ramirez*-recognized harm of "disclosure of private information." *Ramirez*, 594 U.S. at 425. Further, Plaintiff asserts that Defendant's exposure of his sensitive data has resulted in fraudulent activity, supported by a surge in spam communications and an attempted banking breach. Even if these were Plaintiff's only allegations, he would have sufficiently established concreteness at the pleading stage. *Rauhala v. Greater New York Mut. Ins., Inc*., No. 22-1788, 2022 WL 16553382, at *3 (E.D. Pa. Oct. 31, 2022) (denying a motion to dismiss and describing plaintiff's alleged increase in spam calls as a concrete and particularized harm).

In addition to his allegations of misuse, Plaintiff argues that his heightened risk of identity theft also establishes concreteness. I agree. Where a plaintiff advances a substantial risk theory, he can "satisfy concreteness as long as he alleges that the exposure to that substantial risk caused additional, currently felt concrete harms." *Clemens*, 48 F.4th at 155-56. The Third Circuit explained that if, for example, "the plaintiff's knowledge of the substantial risk of identity theft causes him to presently experience emotional distress or spend money on mitigation measures like credit monitoring services, the plaintiff has alleged a concrete injury." *Id.* at 156.

As in *Clemens*, Plaintiff's fear of future identity theft is sufficiently concrete because it is bolstered by presently felt harms. Plaintiff asserts that he has suffered monetary losses, lost time, anxiety, and emotional distress from Defendant's failure to safeguard his data and adequately notify him about the Incident. The Complaint specifies that these losses include out-of-pocket costs from trying to "prevent, detect, and recover[] from identity theft and fraud," as well as ongoing anxiety, sleep disruption, stress, fear, and frustration. Compl. ¶ 62.

Because Plaintiff pleads injuries that are both actual or imminent, concrete, and particularized, Plaintiff sufficiently establishes injury-in-fact.

B. Plaintiff's alleged injuries are fairly traceable to Defendant.

The second prong of the standing inquiry requires a plaintiff to establish that the injury was caused by the challenged action of the defendant, as opposed to an independent action of a third party. *Lujan*, 504 U.S. at 560. Either but-for or concurrent causation will suffice. *See Edmonson v. Lincoln Nat. Life Ins. Co.*, 725 F.3d 406, 418 (3d Cir. 2013) (finding the traceability requirement met "where the conduct in question might not have been a proximate cause of the harm, due to intervening events"); *Aichele*, 757 F.3d 347, 366 (3d Cir. 2014) (explaining that an indirect causal relationship will suffice, so long as there is a fairly traceable connection, even if the direct cause of injury is a third party). Defendant argues that Plaintiff cannot establish traceability, both because it is not clear that any hackers accessed the data within the nine-day period, and because the type of information exposed is not the type of information that would facilitate the attempted bank fraud that Plaintiff asserts. Both arguments fail.

Although there are certainly data breach cases where the known identities and behaviors of hackers might help a plaintiff plead a tighter causal link, a data breach incident need not have a known hacker to merit standing. Here, Plaintiff plausibly alleges that as a result of Defendant's flawed policies and inadequate cyber security training, his sensitive information was exposed for nine days, rendering it susceptible to automatic web scraping bots. Further, Plaintiff alleges that Defendant failed to notify any affected parties of the breach for *nine months*, deeply undercutting Plaintiff's ability to mitigate potential harm. And shortly after Plaintiff's information became available online, in addition to the significant emotional distress, time, and money he allegedly expended, he began experiencing signs of identity theft through attempted bank fraud and a spike in spam calls. It is not difficult to discern a causal link between both Defendant's failure to

safeguard sensitive data and to provide prompt notice and the harms that Plaintiff asserts, even if Plaintiff cannot point to the specific data scraping bot or scam caller at play.

Additionally, it is significant that Defendant failed to notify Incident victims for nine months. *Cf. Clemens*, 48 F.4th at 150-51 (where affected parties were notified immediately and encouraged to take precautionary measures, including enrolling in defendant's complimentary credit-monitoring service); *Roma*, 2024 WL 3678984, at *1 (notifying affected parties after two months); *Rauhala*, 2022 WL 16553382, at *1 (notifying affected parties after four months); *In re Retreat Behavioral Health LLC*, 2024 WL 1016368, at *1 (notifying affected parties after five months). Equity favors relaxation of the pleading standard on traceability where Defendant had knowledge of the breach and does not promptly reveal it, because such delay on its part would have the effect of hindering Plaintiff's ability to plead traceability with the precision Defendant now demands. Had Defendant timely disclosed the Incident, patterns of increased fraudulent activity such as those observed by Mr. LaSalle may have been recognized by other members of the putative class, facilitating identification of further potentially affected individuals. But the lengthy delay necessarily limits the ability of those impacted by the breach to notice a pattern and assert their claims.

Finally, Defendant's simplistic assertion that one cannot attempt to open a fraudulent bank account without access to one's banking information is divorced from reality. As recognized by the Eleventh Circuit, there is "unequivocal damage" that can be done with social security numbers, names, and dates of birth, as this data is some of "the most sensitive personal information possible." *In re Equifax Inc. Customer Data Sec. Breach Litig.*, 999 F.3d 1247, 1257, 1262 (11th Cir. 2021). And it is often the case that cybercriminals and hackers target password protected

accounts using piecemeal sensitive information, such as the names, birthdays, social security records, and more, at issue here.

At this stage of litigation, Plaintiff's allegations that Defendant's failure to safeguard sensitive data and to timely notify victims of the Incident led to resultant fraud, anxiety, and mitigation costs are sufficient to demonstrate traceability. While Defendant may ultimately show, after the opportunity for discovery, that the alleged injuries are not caused by the Incident, it is premature to dismiss Plaintiff's claims on traceability grounds. *See In re Marriott Int'l Inc., Customer Data Security Breach Litig.*, 440 F.Supp.3d 447, 495 (D. Md. 2020) (plaintiffs sufficiently established traceability by asserting that they gave information to the defendant, defendant had a data incident, the scope of the incident was unknown, and the plaintiffs experienced harm).

In sum, at least one plaintiff, Mr. LaSalle, has plausibly alleged that he has suffered an injury in fact, and that those injuries can be fairly traced to Defendant's conduct. *Lujan*, 504 U.S at 560. As Defendant does not contest that Plaintiff's injuries would be redressed by the relief Plaintiff seeks, Plaintiff has therefore plausibly alleged Article III standing.[6]

IV. Conclusion

For the reasons set forth above, Defendant's Motion to Dismiss will be denied. An appropriate order follows.

/s/ Gerald Austin McHugh
United States District Judge

[6] Although not addressed by either party, Plaintiff's claims are redressable. "The injuries caused by a data breach are 'easily and precisely compensable with a monetary reward,'" and Plaintiff's concerns about future harms could be assuaged if Defendant were required to take protective measures or implement new cybersecurity policies. *See Clemens*, 48 F.4th at 157 (citing *Reilly*, 665 F.3d at 45-6).